OGÓLNE ZASADY POSTĘPOWANIA OFERTOWEGO

1. W szczególnie uzasadnionych przypadkach Zamawiający może w każdym czasie, przed upływem terminu składania ofert, zmodyfikować treść dokumentów zawierających istotne warunki zamówienia. Dokonane w ten sposób uzupełnienie przekazane zostanie niezwłocznie wszystkim Wykonawcom.
2. Zamawiający może zwrócić się do Wykonawców o przedłużenie ważności oferty o czas oznaczony.
2. Zmiany albo wycofanie oferty dokonane przez Wykonawcę przed upływem terminu do składania ofert są skuteczne.
3. W toku dokonywania oceny złożonych ofert Zamawiający może żądać udzielenia przez Wykonawców wyjaśnień dotyczących treści złożonych przez nich ofert.
4. Wszystkie informacje zawarte w niniejszym zapytaniu ofertowym są poufne. Wykonawca jest zobowiązany nie ujawniać, nie przekazywać informacji poufnych w sposób pośredni ani bezpośredni osobom trzecim, nie kopiować, nie powielać, ani w inny sposób nie reprodukować, ani nie wykorzystywać ich dla celów innych, niż związanych z zapytaniem ofertowym.
5. Zamawiający nie ponosi żadnej odpowiedzialności ani jakichkolwiek kosztów związanych z przygotowaniem oferty przez Wykonawcę, a w szczególności związanych z przystąpieniem do procesu ofertowego, przygotowaniem **i** złożeniem oferty, negocjacji, przygotowaniami do zawarcia umowy.
7. Zamawiający zastrzega sobie prawo do dowolnego wyboru Wykonawcy.
8. Bezpośrednio po zakończeniu negocjacji, dokonaniu wyboru Zamawiający zawiadamia wybranego Wykonawcę, iż jego oferta została przyjęta oraz przedstawia mu umowę do podpisu. Pozostałych Wykonawców, Zamawiający zawiadamia o dokonaniu wyboru.
9. Zakończenie niniejszego postępowania przetargowego następuje z chwilą zawarcia umowy z wybranym Wykonawcą.
10. Po wykonaniu prac. Wykonawca przeniesie na Zamawiającego autorskie prawa majątkowe.

OPIS SPOSOBU PRZYGOTOWANIA OFERT

1. Oferta powinna zostać przygotowana w języku polskim i przesłana na …… .....
2. Oferta powinna być podpisana przez upoważnionego przedstawiciela Wykonawcy, a wszystkie jej strony parafowane.
3. Wszelkie poprawki w treści oferty muszą być parafowane przez osobę podpisującą Ofertę.

WYMAGANIA WOBEC OFERENTÓW

Doświadczenie Oferenta:

1. Co najmniej 2 wdrożone systemy zarządzania bezpieczeństwem informacji (SZBI) wg standardu PN-ISO/IEC 27001:2014 zakończone w okresie ostatnich 24 miesięcy o wartości minimum 50.000 zł brutto każdy.
2. Co najmniej 1 projekt dostosowania wymagań systemu do Rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych zakończony w okresie ostatnich 48 miesięcy.
3. Co najmniej dwie usługi polegające na przeprowadzeniu audytu bezpieczeństwa systemów teleinformatycznych, w tym testów penetracyjnych aplikacji Web oraz analiz konfiguracji systemów IT pod kątem bezpieczeństwa, przy czym wartość każdej usługi była nie mniejsza niż 20 000 PLN brutto zakończone w okresie ostatnich 48 miesięcy.
4. Co najmniej trzy usługi polegające na przeprowadzeniu szacowania ryzyka w obszarze bezpieczeństwa informacji zgodnie z wymaganiami PN-ISO/IEC 27005:2014 w organizacji posiadającej rozproszoną strukturę, o liczbie zatrudnionych osób nie mniejszej niż 100 zakończone w okresie ostatnich 48 miesięcy.
5. Co najmniej jeden projekt powinien obejmować dostosowanie do wymagań Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych).
6. Z uwagi na charakter usług okresowych dopuszcza się wykazanie projektów, które nadal są prowadzone.
7. W zakresie punktów 1, 2, 3 i 4 wykonane projekty powinny zastać potwierdzone referencjami.

Kwalifikacje Oferenta

Punkt ten określa minimalne kwalifikacje zespołu, który zostanie zaangażowany w proces realizacji zamówienia:

a. Zespół składający się z co najmniej 3 osób, w tym obowiązkowo z Kierownika projektu o wykształceniu wyższym informatycznym, posiadający certyfikat IT Foundation oraz certyfikat audytora wiodącego ISO/IEC 27001 wydany przez akredytowaną jednostkę;
b. W zakresie pozostałych osób zespołu do dyspozycji pozostają następujący członkowie:

- ekspert o wykształceniu wyższym informatycznym, posiadający certyfikat CISSP wydany przez akredytowaną jednostkę,
- ekspert o wykształceniu wyższym prawniczym,
- konsultant, posiadający wykształcenie wyższe i doświadczenie w realizacji projektów z obszaru ochrony danych osobowych, przy czym musi posiadać co najmniej jeden uznany certyfikat z obszaru bezpieczeństwa informacji - CISSP, CISM, CISA lub audytora wiodącego ISO 27001.

Termin wykonania usługi

Realizacja usługi i zakończenie projektu nastąpi do dnia 4.12.2017.

Pozostałe wymagania

1. Zamawiający nie dopuszcza udziału podwykonawców w realizacji zamówienia.

Przedmiot zamówienia

Przedmiotem zamówienia jest usługa polegająca na:

- Ocenie dostosowania systemu zarządzania w ZTM do wymagań RODO - Rozporządzenia Parlamentu Europejskiego i Rady 2016/679 z dnia 27 kwietnia 2016 w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych zwane RODO)
- Ocenie dostosowania systemu zarządzania w ZTM do wymagań Rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 w sprawie KRI - Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych w Zarządzie Transportu Miejskiego w Poznaniu (zwane KRI)
- Ocenie dostosowania Systemu Zarządzania Bezpieczeństwem Informacji w oparciu o normę PN-ISO/IEC 27001:2014 w Zarządzie Transportu Miejskiego w Poznaniu
- Opracowanie koncepcji wdrożenia Systemu Zarządzania Bezpieczeństwem

Informacji w oparciu o normę PN-ISO/IEC 27001:2014 w Zarządzie Transportu Miejskiego w Poznaniu

Zakres wymaganych prac jest następujący:

ETAP I DIAGNOZA PRZEDWDROŻENIOWA (Audyt zerowy)

1.1. Cel audytu zerowego

Audyt zerowy w Zarządzie Transportu Miejskiego, w siedzibie przy ul. Matejki 59 w Poznaniu oraz we wszystkich pozostałych lokalizacjach ZTM na terenie miasta Poznania, którego celem jest:

- Weryfikacja poziomu spełnienia wymagań Rozporządzenia Parlamentu Europejskiego i Rady 2016/679 z dnia 27 kwietnia 2016 w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE zwanego dalej RODO
- Weryfikacja poziomu spełnienia wymagań Rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych w Zarządzie Transportu Miejskiego w Poznaniu, zwanego dalej KRI
- Weryfikacja poziomu spełnienia wymagań normy PN-ISO/IEC 27001:2014 przez ZTM, w tym ocena skuteczności funkcjonujących zabezpieczeń technicznych, organizacyjnych i prawnych stosowanych w ZTM, w obszarach określonych załącznikiem A do ww. normy
- Przeprowadzenie inwentaryzacji zbiorów danych osobowych
- Przeprowadzenie inwentaryzacji aktywów informacyjnych związanych z bezpieczeństwem informacji
- Opracowanie koncepcji przystosowania organizacji do wymagań ISO 27001:2014, RODO oraz KRI, w tym przedstawienie szczegółowego harmonogramu prac.

1.2. Zakres audytu zerowego

Zakres prac podczas audytu zerowego będzie obejmował co najmniej:

1.2.1. Zapoznanie się ze strukturą organizacyjną ZTM;

1.2.2. Analizę i ocenę dokumentacji w zakresie:

- bezpieczeństwa informacji,
- ochrony danych osobowych
- zarządzania ryzykiem

w tym polityk, procedur, zarządzeń, instrukcji, regulaminów wewnętrznych, umów powierzenia danych osobowych zawieranych przez ZTM, dokumentacji dotyczącej zarządzania ryzykiem, rejestrów zbiorów danych osobowych, dokumentacji szkoleń, identyfikacji procesów oraz innych dokumentów, które Zamawiający udostępni Wykonawcy do analizy. Zamawiający zastrzega sobie prawo do udostępnienia wyłącznie wybranej dokumentacji poza jego siedzibę w formie ustalonej z Wykonawcą;

1.2.3. Wywiady z wytypowanymi przez Zamawiającego pracownikami poszczególnych komórek organizacyjnych (do rozmowy wytypowanych zostanie minimum 40% pracowników ZTM) w zakresie niezbędnym do ustalenia poziomu stosowania wymagań określonych przez Rozporządzenie RODO, KRI i normę PN-ISO/IEC 27001:2014 oraz wewnętrzne uregulowania ZTM;

1.2.4. Obserwacje działań i zachowań pracowników w tym próba pozyskania informacji (danych osobowych) – rozmowy z pracownikami, badania socjotechniczne. Uzyskana wiedza posłuży do przygotowania szkoleń o odpowiednim zakresie.

1.2.5. Ocenę stanu bezpieczeństwa fizycznego siedziby ZTM oraz wszystkich lokalizacji (budynki oraz pomieszczenia)

1.2.6. Wizję lokalną kluczowych miejsc przetwarzania danych osobowych

1.2.7. Analizę procesu zarządzania ciągłością działania w kontekście bezpieczeństwa informacji w tym przeprowadzenie identyfikacji zagrożeń)

1.2.8. Przeprowadzenie inwentaryzacji zbiorów danych osobowych (cel, zakres, podstawa prawna przetwarzanych danych osobowych, systemy przetwarzające dane osobowe, podmioty, którym dane osobowe są powierzane)

1.2.9. Inwentaryzację aktywów/grup aktywów związanych z bezpieczeństwem informacji

1.2.10. Analizę bezpieczeństwa systemów teleinformatycznych, ze szczególnym uwzględnieniem systemów w których przetwarzane są dane osobowe

1.2.11. Analizę procesu zarządzania incydentami naruszenia ochrony danych osobowych

1.2.12. Audyt u wybranych dwóch podmiotów w zakresie realizacji umowy powierzenia danych osobowych pomiędzy ZTM a danym podmiotem mających siedzibę w Poznaniu lub gminach ościennych

1.2.13. Wykonawca zobowiązany jest do opracowania planu audytu zerowego i przekazaniu dokumentu do akceptacji Zamawiającego. Plan audytu powinien zawierać co najmniej:

- Cel, zakres i kryteria audytu
- Harmonogram działań audytowych w poszczególnych komórkach organizacyjnych i lokalizacjach
- Wykaz audytorów
- Podpisy sporządzającego i akceptującego dokument

Plan audytu będzie podlegał akceptacji przez Zamawiającego.

1.2.14. Wykonawca jest zobowiązany do opracowania raportu z przeprowadzonego audytu zerowego zawierającego:

- Cel, zakres i kryteria audytu
- Szczegółowy opis przeprowadzonych prac
- Szczegółowy opis poziomu spełnienia każdego z wymagań normy PN-ISO/IEC 27001:2014 opisanych w załączniku A do niniejszej normy
- Wykaz stwierdzonych niezgodności w odniesieniu do kryteriów audytu: wymagań RODO, KRI oraz wymagań normy PN-ISO/IEC 27001:2014
- Rekomendacje w zakresie proponowanego sposobu wyeliminowania wykrytych niezgodności w odniesieniu do wymagań RODO, KRI oraz wymagań normy PN-ISO/IEC 27001:2014
- Podsumowanie i wnioski.

1.2.15. Raport, o którym mowa w punkcie 1.2.14 Wykonawca przekaże Zamawiającemu w formie papierowej, w liczbie 1 egzemplarza oraz w formie elektronicznej jako zaszyfrowany plik na podany przez Zamawiającego e-mail. Klucz zostanie przekazany w sposób uzgodniony z Zamawiającym. Forma elektroniczna raportów będzie przygotowana w plikach edytowalnych w formatach docx, pptx, xlsx.

1.2.16. Zamawiający zastrzega sobie prawo do wnoszenia uwag do przekazanego przez Wykonawcę raportu, o którym mowa w pkt 1.2.14. w terminie do 14 dni.

1.2.17. Wykonawca zobowiązany jest do uwzględnienia w raporcie wniesionych przez Zamawiającego uwag do raportu, o którym mowa wyżej w terminie do 14 dni.

1.2.18. Najważniejsze wnioski z audytu Wykonawca jest zobowiązany przedstawić kierownictwu ZTM w formie prezentacji multimedialnej.

ETAP II WYKONANIE AUDYTU TECHNICZNEGO ORAZ SOCJOTECHNICZNEGO

1. Przeprowadzenie audytu technicznego IT zostanie zrealizowane zgodnie z załącznikiem nr 1 (audyt techniczny) do OPZ.
2. Testy socjotechniczne* zostaną zrealizowane zgodnie z dostarczonymi przez wykonawcę scenariuszami w zakresie :
    a. 2 prób dostępu fizycznego
    b. 3 prób dostępu e-mailowego/elektronicznego
    c. 1 próby dostępu telefonicznego

4. Opracowanie szczegółowego raportu ze znalezionymi podatnościami i opisem.
5. Wykonanie re-testów znalezionych podatności z punktu 1 i punktu 2

* Wykonawca zaproponuje scenariusze testowe na etapie projektów

ETAP III SZKOLENIE ZESPOŁU WDROŻENIOWEGO

2.1. Wykonawca po zakończeniu etapu I i II tj. po przeprowadzeniu audytu zerowego i audytu technicznego zobowiązany jest do przygotowania planu i poprowadzenia szkolenia wstępnego dla zespołu wdrożeniowego powołanego przez ZTM oraz szkolenia dla pracowników działu informatycznego obejmującego omówienie podatności zidentyfikowanych podczas audytu technicznego

2.2. Szkolenie dla Zespołu wdrożeniowego swoim zakresem będzie obejmowało co najmniej:

2.2.1. Wprowadzenie do problematyki RODO, KRI i SZBI

2.2.2. Omówienie wymagań normy PN-ISO/IEC 27001:2014

2.2.3. Omówienie wyników audytu zerowego i technicznego

2.2.4. Wprowadzenie do zarządzania ryzykiem

2.2.5. Szkolenie dla Zespołu wdrożeniowego będzie odbywało się w siedzibie Zamawiającego i będzie trwało 2 dni, po 6 godzin zegarowych każdego dnia

2.3. Szkolenie dla pracowników działu informatycznego swoim zakresem będzie obejmowało co najmniej:

2.3.1. Wprowadzenie do problematyki RODO, KRI i SZBI

2.3.2. Omówienie wymagań normy PN-ISO/IEC 27001:2014

2.3.3. Omówienie podatności zidentyfikowanych podczas audytu technicznego

2.4. Szkolenie dla pracowników działu informatycznego będzie odbywało się w siedzibie Zamawiającego dla 2 grup po 4 godziny zegarowe

2.5. Wykonawca przekaże Zamawiającemu plan szkoleń, o którym mowa w pkt 2.2. i 2.3. najpóźniej na 7 dni przed planowanym terminem rozpoczęcia szkolenia

2.6. Wykonawca zobowiązany jest do przygotowania materiałów szkoleniowych oraz imiennej listy uczestników szkolenia zawierającej informacje o liczbie godzin, obecności uczestników, podpis uczestnika szkolenia i podpis prowadzącego szkolenie

2.7. Wykonawca przekaże Zamawiającemu materiały szkoleniowe i prezentację razem z planem szkolenia, najpóźniej na 7 dni przed planowanym terminem rozpoczęcia szkolenia

2.8. Zamawiający zastrzega sobie prawo do wnoszenia uwag do przekazanych przez Wykonawcę materiałów szkoleniowych oraz planu szkolenia, w tym do zmiany planowanego terminu szkolenia

2.9. Wykonawca zobowiązany jest do uwzględnienia uwag przekazanych przez Zamawiającego, o których mowa w pkt 2.8, w terminie 2 dni roboczych.

2.10. Po zakończeniu szkolenia Wykonawca wyda certyfikaty udziału w szkoleniu.